

PH NL
010532 WO
PCT

MAT.
DOSSIER

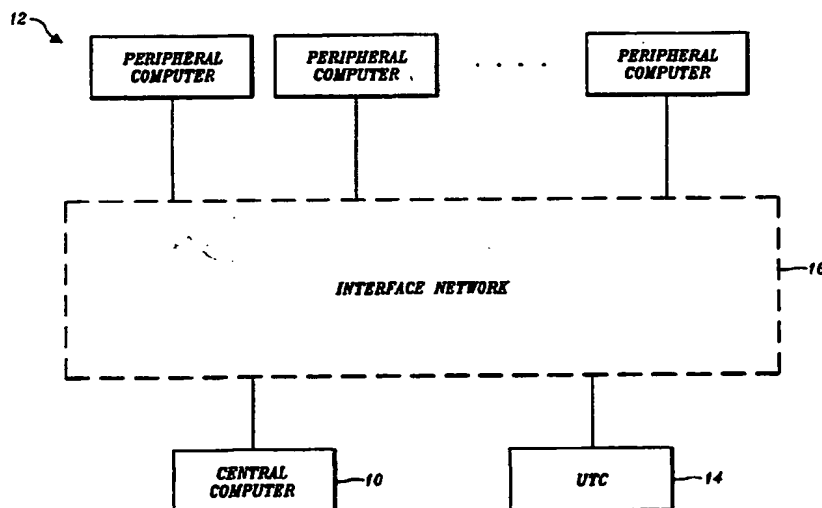
WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : G06F 7/02, H04L 9/32		A1	(11) International Publication Number: WO 95/15522
			(43) International Publication Date: 8 June 1995 (08.06.95)
(21) International Application Number: PCT/US94/13360 (22) International Filing Date: 18 November 1994 (18.11.94) (30) Priority Data: 08/160,938 2 December 1993 (02.12.93) US (71) Applicants: SCHEELE, Drew [US/US]; 201 West Lake Rosinger Road, Snohomish, WA 98290 (US). MARTONICK, Michael [US/US]; Suite 240, 765 Wesley Street, Arlington, WA 98223 (US). LEVI, Dean, F. [US/US]; 5210 - 122nd Street Southeast, Everett, WA 98208 (US). (71)(72) Applicant and Inventor: JONES, Robert, F. [US/US]; 1701 - 121st Street Southeast #M204, Everett, WA 98208 (US). (74) Agent: KINDNESS, Gary, S.; Christensen, O'Connor, Johnson & Kindness, Suite 2800, 1420 Fifth Avenue, Seattle, WA 98101 (US).		(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LR, LT, LU, LV, MD, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), ARIPO patent (KE, MW, SD, SZ). Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>	

(54) Title: DIGITAL DATA VERIFICATION SYSTEM



(57) Abstract

A computer file verifier for verifying computer files as authentic is provided. The computer file verifier is implemented on a multi-computer system including one or more peripheral computers (12), a central computer (10) including secured memory, and an interface network (16) interconnecting the computers. The peripheral computers (12) are used to create computer files (24). If a computer file (24) is to be later verified, a peripheral computer (12) generates a fingerprint of the computer file (24). The fingerprint is then stored in the secured memory of the central computer (10). To verify the content of the file, the peripheral computer (12) regenerates the fingerprint and the regenerated fingerprint is compared to the fingerprint stored on the central computer (10). If the fingerprints match, the content of the computer file is verified as unaltered. The date and time of creation and the author of the computer file (24) is preferably stored in the secured memory of the central computer (10) as well, so that this information can also be verified.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgyzstan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

DIGITAL DATA VERIFICATION SYSTEM

Field of the Invention

This invention relates to verifying digital data and, more particularly, verifying the authenticity of digital computer files.

5

Background of the Invention

Despite the ease with which information can be created and stored on today's computers, computers are not used in many applications because there is no acceptable way to verify computer files. For example, in the medical profession physicians maintain patient records, i.e., charts, using nonerasable pen and paper. The physician initials and dates each entry made in a patient's chart. Because such entries cannot be altered without detection, they are considered authentic and therefore acceptable in judicial proceedings. Another example in which pen and paper records are principally used is technical and scientific research. Typically, a researcher maintains a "lab notebook" to track testing and research developments. Each entry is dated and initialed. These lab notebooks are considered admissible evidence to prove, for example, a date of invention or reduction to practice. As a result, to date, many medical, research and other records must be stored in "hard copy" form. Computer storage has generally been considered unacceptable because, in the past, electronic files have been too easy to alter without detection.

20

In the past, computers have been relatively large and cumbersome to use so that the inability to use computers for such purposes as storing verifiable medical and research records has not been a very significant problem. However, computers have become much easier to use and much more portable, and further improvements are expected in the future. Accordingly, the use of computers in areas where data

-2-

authenticity is a requirement is increasingly desirable. Indeed, laptop, notebook and palmtop computers are now available and are ideal for creating patient charts, recording research progress, and recording financial data and transactions.

5 Unfortunately, there are no presently available computer data verification systems that provide an acceptable indication of authenticity and veracity. There are techniques to make computer files noneditable, i.e., read-only. For example, many computer programs include read-only files that contain informational text for the user. Unfortunately, the read-only security techniques presently available can be easily defeated. An inherent problem with such systems is that because the read-only
10 techniques can be easily defeated, the security of each computer storing important files must be closely monitored so that no one is able to modify the files on the computer.

What is needed is a simple verification system that verifies the authenticity (i.e., content, author, and date and time of creation) of computer files. The system
15 should be inexpensive and should not require closely monitoring the security of the computers on which the files are created and stored. The present invention fulfills these and other needs as described in full detail herein.

Summary of the Invention

In accordance with this invention, a system for verifying computer files as
20 authentic is provided. The verification system includes a central computer that can be accessed by a plurality of peripheral computers via an interface network. Users create computer files via the peripheral computers, e.g., a desktop personal computer, a laptop computer, a palmtop computer, etc. Methods in accordance with this invention are performed on the peripheral computers and the central computer to
25 "fingerprint" a file after it is created. This way the file can be later verified to determine whether the file has been altered since it was fingerprinted. In particular, after a user creates a file on a peripheral computer, the user can fingerprint the file for later verification. To fingerprint a file, the peripheral computer first calculates a fingerprint using a technique that produces a fingerprint that is unique to the data
30 contained in the file. The peripheral computer then accesses the central computer and the central computer stores the file fingerprint. Later, to verify the content of a file stored on a peripheral computer, the fingerprint of the file is recalculated using the same technique. The recalculated fingerprint is then compared to the fingerprint stored on the central computer. If the fingerprints match, the file is verified as
35 unaltered. On the other hand, if the fingerprints do not match, then one knows that the file has either been altered or corrupted.

-3-

In accordance with further aspects of the invention, when the file is fingerprinted, the file is also date and time stamped. In particular, the central computer includes a clock that provides the date and time at which the file is fingerprinted. The date and time is then stored in the central computer along with the fingerprint. The date and time is also stored along with the file on the peripheral computer. Then, when verifying the file, the date and time stored with the file on the peripheral computer is verified along with the fingerprint by comparing the date and time with that stored on the central computer.

In accordance with further aspects of the invention, the author of the file must identify himself before the file is fingerprinted. The central computer then keeps a record of the author along with the fingerprint and date and time stamp of the file. In this way, the author of the file can be verified. In one preferred embodiment, the author identifies himself by entering a previously assigned password. The central computer verifies the password before fingerprinting and date and time stamping the file. The fingerprint and date and time stamp are stored in a database assigned exclusively to the author (i.e., user or subscriber), thereby maintaining a record of the file's author.

In accordance with further aspects of the invention, the fingerprinting of a file includes calculating the cyclic redundancy check (CRC) value for the file. In accordance with still further aspects of the invention, the fingerprint also includes the size of the file.

In accordance with still further aspects of the invention, the system includes the ability to store complete files on the central computer by downloading the files from a peripheral computer. This way, the file can be deleted on the peripheral computer to free up memory, and then uploaded from the central computer when needed. Also, if a file on a peripheral computer becomes corrupted, the original file can be uploaded from the central computer if it was previously stored on the central computer.

As will be appreciated from the foregoing brief summary, a system for verifying computer files is provided by this invention. A central computer is used to store fingerprints of files created on various peripheral computers. To verify the content of a file as unaltered, the fingerprint of a file stored on a peripheral computer is recalculated and then compared to the fingerprint stored on the central computer. If the fingerprints match, the content of the file is verified as unaltered. The system also includes the ability to date and time stamp files. The date and time stamp is stored along with the fingerprint on the central computer so that the date and time of

-4-

creation of the file can be later verified. The system also includes the ability to record on the central computer the file's author so that the author of the file can be verified as well. By tightly maintaining the security of the central computer, the fingerprint, author, and date and time stamp verification data are preserved. This way, despite lax security on numerous peripheral computers, computer files created on the peripheral computer can be later verified. In other words, a high security of data on numerous computers is achieved by simply maintaining the security of a single computer, namely, the central computer. As a result, a relatively low cost system for verifying the authenticity (i.e., content, author, and date and time of creation) of computer files is provided. It will be further appreciated that the invention also allows the downloading of files from a peripheral computer to the central computer so that the central computer can store a file for later retrieval (i.e., uploading) in case the file is either deleted or corrupted on one of the peripheral computers. As a result, computers can be used to create records required to have a high level of authenticity and veracity such as patient medical records, research laboratory records, and financial records.

Brief Description of the Drawings

The foregoing aspects and many of the attendant advantages of this invention will become more readily appreciated as the same becomes better understood by reference to the following detailed description, when taken in conjunction with the accompanying drawings, wherein:

FIGURE 1 is a system block diagram of a multi-computer system structured in accordance with the present invention;

FIGURE 2A is a block diagram illustrating the types of files, including document files, stored on a peripheral computer in accordance with the invention, and FIGURE 2B shows a document file in more detail;

FIGURE 3A is a block diagram illustrating the types of files, including subscriber databases, stored on a central computer in accordance with the invention, and FIGURE 3B shows a subscriber database in more detail;

FIGURES 4A-4D show a composite flow diagram illustrating in part how the invention operates; and

FIGURE 5 contains a flow diagram illustrating in part the operation of a peripheral computer in accordance with the invention.

Detailed Description of the Preferred Embodiment

FIGURE 1 is a system block diagram of multiple computers configured and interconnected in accordance with the invention. The verification system includes a

-5-

central computer 10, multiple peripheral computers 12, and a universal time clock (UTC) 14, all interconnected via an interface network 16. The peripheral computers 12 are computers on which computer files are created by an author (i.e., user or subscriber of the verification system). The peripheral computers 12 can take many forms, including personal computers such as desktop computers, laptop computers, notebook computers, or palmtop computers. In accordance with the invention, after a file is created on a peripheral computer 12, the file can be "fingerprinted," so that the content of the file can be verified as unaltered at a later time. In particular, the peripheral computer uses a particular technique to generate a fingerprint that is unique to the particular data stored in the file. The peripheral computer 12 then accesses the central computer 10 via the interface network 16 and the fingerprint is stored on the central computer. When verification of the file is needed, the peripheral computer recalculates the fingerprint using the same technique, and the recalculated fingerprint is then compared to the fingerprint stored on the central computer. If the fingerprints match, the file content is verified as unaltered since the file was fingerprinted.

The verification system provided by the invention could be offered by a verification service company. For example, the service company would have the central computer 10 and would provide software for various users or subscribers for use on their own computers, i.e., peripheral computers 12. The peripheral computers would access the central computer 10 via the interface network 16. For example, the interface network could include modems on each of the peripheral computers, a modem on the central computer, and a telephone network to interconnect the modems. The interface network 16 could also be a commonly used wide area network. The verification service company would tightly monitor the security of the central computer 10 so as to maintain the veracity of file fingerprints stored on the central computer 10. Alternatively, a business having many computers could implement the data verification system shown in FIGURE 1 in-house. The peripheral computers 12 would be computers used throughout the business, and the central computer 10 would be a computer for verifying the files on the peripheral computers. The interface network 16 could then be some form of local area network.

In addition to fingerprinting files created on the peripheral computers 12, the central computer 10 preferably date and time stamps each file. This way, the date and time of creation, as well as the content of a file can be later verified. The central computer accurately and robustly tracks the date and time so that files can be properly date and time stamped. In one preferred embodiment, the central computer includes

-6-

an internal clock and a battery backup as is commonly available in today's computers. The central computer 10 periodically updates its internal clock by comparing its time with the universal time clock 14, which maintains, for example, Greenwich mean time.

Preferably, the author of a file cannot gain access to the central computer 10 to have a file fingerprinted and date and time stamped unless the author properly identifies himself. The central computer verifies that the author is a user or subscriber of the verification system and then maintains a record of the author along with the file fingerprint and date and time stamp. In this way, the author of the file can be later verified. In one preferred embodiment, this is accomplished by assigning a unique password to each user or subscriber. The user must correctly enter the password to gain access to the central computer 10. The central computer 10 stores a subscriber database for each user. When a file is fingerprinted and date and time stamped for a particular user identified by their password, the file fingerprint and date and time stamp is stored in the subscriber database assigned to that user. As a result, the file's author is recorded, namely, the user associated with the subscriber database.

The central computer also preferably has the ability to store copies of files created on the peripheral computers 12. In particular, a peripheral computer 12 can download a copy of a file to the central computer 10 via the interface network 16. This way, if a file is deleted from a peripheral computer or if a file on the peripheral computer is altered or corrupted, the copy can be uploaded from the central computer 10.

FIGURES 2 and 3 illustrate the type of files stored on the peripheral computers 12 and the central computer 10. The peripheral computer 12 includes memory 18 that can be formed of any presently available memory or storage devices, e.g., random access memory (RAM), disc drives, laser discs, etc. As shown in FIGURE 2A, the memory 18 stores, among other things, document files 22 and a program 20 referred to as the Digital Data Verifier Peripheral (DDVP). The DDVP program 20 is programmed according to the invention to work in conjunction with the central computer to provide verification of user created documents. A document file 22 is created by the verification system upon fingerprinting a user created document 24 by appending a document activity log (DAL) 28 to the user created document 24. A document file 22 is shown in greater detail in FIGURE 2B. The document 24 is the computer file created by the user to contain the data 27, and the document activity log 28 contains file identification information 25 assigned to the document 24 and an ongoing record of activity 26 performed on the document file 22.

-7-

Upon creation by the verification system, the document files 22 are preferably stored in a section of the memory 18 that is configured to be noneditable, i.e., a nonedit archive 30. The nonedit archive provides a first level of security against file tampering and, just as importantly, prevents a user from inadvertently altering a fingerprinted file. The nonedit archive can be formed using techniques presently well known in the computer arts area. Unfortunately, the nonedit attribute of the archive 30 formed with present techniques can be easily defeated by persons highly skilled in computers, so that storing files in the nonedit archive 30 does not provide a sufficient level of file verification. Accordingly, in accordance with the present invention, a fingerprint for each document is stored on the central computer 10 -- the security of which is highly maintained -- to provide an acceptable level of file verification.

FIGURE 3A shows the usage of memory 32 included in the central computer 10. The memory 32 can be formed of any presently available memory or storage devices. A portion of the memory 32 is used to store a program 34 referred to as the Digital Data Verifier Central (DDVC), which is programmed in accordance with the invention to provide file verification in conjunction with the DDVP program 20. Another portion 36 of the memory 32 stores subscriber databases 38, one for each subscriber or user. The composition of a subscriber database 38 is shown in greater detail in FIGURE 3B. As shown, a subscriber database 38 includes an account log 40 that stores subscriber information and a record of system usage, which can be used, for example, for purposes of billing the subscriber. A subscriber database 38 also includes document data 42 and downloaded documents 44. The document data 42 includes a document record 46 for each user created document 24 entered into the verification system, i.e., a document record 46 for each document file 22. The document records 46 include file fingerprints, date and time stamps, as well as other data as described in detail hereinafter. The downloaded documents 44 include copies 48 of selected document files 22 stored on a peripheral computer 12.

The operation of the DDVP program 20 and the DDVC program 34 is illustrated by the flow diagrams shown in FIGURES 4A-4D and FIGURE 5. In particular, FIGURE 5 illustrates a portion of the steps of the DDVP program 20 performed on a peripheral computer, and FIGURES 4A-4D illustrate steps performed by the combination of the DDVC program 34 and the DDVP program 20, respectively on the central computer and a peripheral computer. As seen for example in FIGURE 4A, the flow diagrams shown include oval blocks, such as the block 50, that indicate the start and end of a program; rectangular blocks, such as the block 54,

-8-

that illustrate an operational step; diamond blocks, such as the decision diamond 52, that indicate a decision step that determines which subsequent steps are performed; and eight-sided blocks, such as the page connector 58, which indicate that program flow is returning from or going to a portion of a flow diagram illustrated in another figure.

FIGURE 5 illustrates the high level operation of the DDVP program 20 on a peripheral computer. When a user wants to perform one of the functions provided by the verification system, the DDVP program 20 is started at the block 160. The program first determines whether or not the DDVP software has been installed, as indicated by the decision diamond 162. If the software has not been installed, it is installed as indicated by the block 164 and then the nonedit archive 30 shown in FIGURE 2A is established, as indicated by the block 166. If the DDVP software is already installed, or after installing the software as indicated by the blocks 164 and 166, program control continues at the decision diamond 168, where a determination is made whether the user wants to review a previously fingerprinted (FP'ed) document 24, i.e., review a document file 22.

If the user does not wish to review a previously fingerprinted document, a determination is then made at the decision diamond 170 to query whether the user wants to fingerprint a new document or verify, download or upload a previously fingerprinted document. If the user chooses to fingerprint a new document, the user first selects the document 24 to be fingerprinted, as indicated at the block 172. The DDVP program then copies the selected document 24 to the nonedit archive 30, establishes a document ID number, and attaches a document activity log 28 to the document 24, so as to create a document file 22, as indicated at the block 174. Next, the peripheral computer 12 contacts the central computer 10 via the interface network 16, as indicated at the block 176. Program control then continues in FIGURE 4A, as indicated by the page connector 178, to fingerprint (and date and time stamp) the file, as hereinafter described. If, at the decision diamond 170, the user instead chooses to verify, upload or download a previously fingerprinted document, the step at the block 180 is performed to allow the user to select the desired document file 22 by entering the file's identification number. Thereafter, contact is established with the central computer (indicated at the block 176), and program control continues in FIGURE 4A (indicated by the page connector 178) to verify, upload or download the selected file, as hereinafter described.

If, at the decision diamond 168, the user requests to review a document file 22, the steps 182, 184, and 186 are performed. First, the user selects the

-9-

identification number ID# of the document file 22 they want to review, as indicated at the block 182. The user is then able to review the document file 22 on a computer screen of the peripheral computer and/or print the document file 22, as indicated by the block 184. This activity is recorded in the document activity log 28 of the document file 22, as indicated by the block 186. The user is then given the option to exit the DDVP program, as indicated by the decision diamond 188. If the user decides to exit the DDVP program, the program is terminated at the block 190. On the other hand, if the user does not wish to terminate the DDVP program, program control loops back to the decision diamond 168, where the user is again given the choice to review a fingerprinted document.

The starting of the DDVC program 34 on the central computer 10 begins at the block 50, as shown in FIGURE 4A. Operation begins with the steps 52, 54, and 56 to maintain the clock on the central computer and to determine whether a new user has come on line. At the decision diamond 52, a determination is made as to whether the central computer clock should be recalibrated. As shown, preferably, the clock is recalibrated every midnight, and whenever a power interruption, system reinitialization, or system tampering occurs. If recalibration is needed, the clock is recalibrated as indicated by the block 54. In one preferred embodiment, the clock is calibrated by contacting a universal time clock 14 via the interface network 16, as shown in FIGURE 1. The universal time clock 14 preferably maintains Greenwich mean time (GMT). After recalibrating the clock, the step at the decision diamond 52 is again performed. Unless some intervening event has occurred, the clock will not need recalibrating and program control will continue at the decision diamond 56. Similarly, if upon first execution of the step 52, the clock does not need recalibrating, program flow continues at the decision diamond 56.

At the decision diamond 56, a determination is made as to whether a user at a peripheral computer has just come on line, i.e., has established contact with the central computer. A user coming on line is illustrated in FIGURE 4A by the page connector 58, which is reached from the previously described steps shown in FIGURE 5, in particular, from the page connector 178. If a determination is made that a new user is not on line, program control loops back to the decision diamond 52 to again determine whether the clock needs to be recalibrated and then to determine whether a new user has come on line. This sequence repeats until a new user comes on line. When a new user comes on line, the hereinafter described log-in steps indicated by the blocks 60-76 are performed. Concurrently, program control loops back to the decision diamond 52 to again determine whether the clock needs to be

-10-

recalibrated and then to determine whether another user has come on line. In this manner, the central computer can support several users concurrently. The concurrent operation can be accomplished by either time sharing a single processor of the central computer or by using multiple processors in parallel, or by other techniques currently known by those skilled in the computer art area.

When at the decision diamond 56 a determination is made that a new user is on line, the log-in steps 60-76 are performed. First, as indicated by the decision diamond 60, a determination is made as to whether the peripheral computer has successfully connected to the central computer. This determination mainly involves determining whether the connection between the peripheral computer 12 and the central computer 10, via the interface network 16, is proper. For example, if the interface network includes modems and a telephone network, the test would include determining whether the modem types and settings are compatible. If the connection is not valid, the user is logged off at the block 78 in FIGURE 4B, which is reached through the page connector 62 in FIGURE 4A and the page connector 80 in FIGURE 4B. If, on the other hand, the connection between the peripheral computer and central computer is satisfactory, the central computer determines whether correct DDVP software, registered to a valid user, is installed on the peripheral computer, as indicated by the decision diamond 64. If the DDVP software is not correct, e.g., an incorrect version, or if the software is not registered to a valid user, a message indicating such is sent to the peripheral computer, as indicated at the block 66, and then the user is logged off at the block 78, which is reached through the page connectors 62 and 80.

On the other hand, if the DDVP software is determined to be proper at the decision diamond 64, the user password is then checked by steps 68-74. The user is given three chances to correctly enter their password. First, at the block 68, a counter #TRIES is set to zero. After the user enters their password, the central computer determines whether the password is correct, as indicated at the decision diamond 70. If the password is not correct, the central computer increments the counter #TRIES, as indicated at the block 72. If the counter #TRIES is not yet equal to three, as determined at the decision diamond 74, then the user is allowed to reenter their password and the password is again checked at the decision diamond 70. If the user is not able to enter their password correctly within three tries, the counter #TRIES reaches three and the determination at the decision diamond 74 causes program control to go to the block 76. At the block 76, a message is sent to the peripheral

-11-

computer to inform the user of the incorrect password. The user is then logged off at the block 78, reached through the page connectors 62 and 80.

If the user is able to successfully enter their password, program control flows from the decision diamond 70 to FIGURE 4B as indicated by the page connectors 82 and 84, respectively in FIGURE 4A and FIGURE 4B. In FIGURE 4B, a determination is first made at the decision diamond 86 as to whether the user wants to fingerprint or verify a document. If the user requested to fingerprint or verify a document, the hereinafter described steps shown in FIGURE 4C are performed, as indicated by the page connector 88. On the other hand, if the user does not want to fingerprint or verify a document, the hereinafter described steps shown in FIGURE 4D are performed to either download or upload a document, as indicated by the page connector 90. After either performing the steps shown in FIGURE 4C or the steps shown in FIGURE 4D, program control returns to FIGURE 4B to execute the step at the decision diamond 92, where a determination is made as to whether the user wants to terminate communication with the central computer. If the user does not want to terminate communication, program control loops back through the blocks 170', 172' and 174' or 170' and 180' to the decision diamond 86 to again determine whether the user wants to fingerprint or verify a file or download or upload a file. The steps 170', 172', 174' and 180' are identical to the steps 170, 172, 174 and 180, shown in FIGURE 5. As described with reference to FIGURE 5, these steps allow the user to select a file for fingerprinting or for verifying, uploading or downloading. If, on the other hand, a determination is made at the decision diamond 92 that the user wants to end communication, the user activity, e.g., the user connect time, is stored in the account log 40 of the subscriber database 38 shown in FIGURE 3B (indicated at the block 94). The user is then logged off at the block 78 and the DDVP program control returns to FIGURE 5, as indicated by the page connector 95. The DDVP program continues from the page connector 179 in FIGURE 5 to the step at the decision diamond 188, where the user is given the option of either terminating the DDVP program or performing further activity, as previously described.

In FIGURE 4B, when a determination is made at the decision diamond 86 that a user wants to fingerprint (FP) or verify a document the steps shown in FIGURE 4C are performed. In particular, to fingerprint (and date and time stamp) a file, the steps 98 and 100 flowing from the page connector 96 are performed. At the block 98, the peripheral computer determines a fingerprint for a user selected document 24 using a preselected technique that produces a fingerprint unique to the

-12-

content of the document. It will be recalled that the user selects the document to be fingerprinted at the block 172 in FIGURE 5 (or at the block 172' in FIGURE 4B). In one particular embodiment, the fingerprint calculated at the block 98 in FIGURE 4C includes the cyclic redundancy check (CRC) value of the file. The algorithm for
5 calculating the CRC value of a file is well known in the computer art and is commonly used for data communication. The fingerprint may also include the size of the document, as indicated in the block 98.

Next, as indicated at the block 100, the fingerprint and other information are stored in the subscriber database 38 assigned to the user. In particular, a document
10 record 46 as shown in FIGURE 3B is created. The fingerprint of the document, including the document's CRC and size in one preferred embodiment, is stored in this record. The present date and time is also determined by reference to the clock on the central computer, and this date and time is stored in the document record 46 so as to date and time stamp the document. The identification number ID# established by the
15 step at the block 174 in FIGURE 5 (or at the block 174' in FIGURE 4B) is also stored in the document record 46 to identify the record. As the block 100 indicates, the peripheral computer stores the document CRC, the document's size, and the date and time in the document activity log 28 of the document file 24, as shown in FIGURE 2B. After performing the step 100, fingerprinting and date and time
20 stamping of the file is complete, and program control returns via the page connector 102 to FIGURE 4B at the page connector 88.

After a user has fingerprinted one or more files, the user can then verify the file at a later point in time. To verify a file, the steps 106-118 after the page connector 104 in FIGURE 4C are performed. First, as indicated at the block 106, the
25 central computer searches the user's subscriber database 38 for the document selected by the user (at the block 180 in FIGURE 5 or at the block 180' in FIGURE 4B) and retrieves the information recorded in the corresponding document record 46. The peripheral computer then recalculates the CRC and size of the document 24 archived on the peripheral computer, as indicated by the block 108. The peripheral computer
30 also retrieves the date and time stamp stored in the document activity log 28 attached to the document 24. The central computer then compares the CRC, file size, and date and time stamp determined by the peripheral computer to the corresponding verification data stored in the subscriber database 38 on the central computer, as indicated at the block 110. At the decision diamond 112, a query is then made as to
35 whether the verification data match. If the data match, the document 24 is valid (i.e., verified) and this determination is recorded in the document activity log 28 on the

-13-

peripheral computer and in the document record 46 in the subscriber database 38 on the central computer, as indicated by the block 114. Thereafter, program control is returned via the page connector 102 to FIGURE 4B at the page connector 88.

5 If, however, at the decision diamond 112 in FIGURE 4C, a determination is made that the verification data do not match, the document 24 is invalid and a corresponding error message is logged in the document activity log 28 on the peripheral computer and in the document record 46 in the subscriber database on the central computer, as indicated at the block 116. Thereafter, at the decision diamond 118, the user is given the option to retry file verification. If the user requests
10 to retry verification, program control loops back to the block 106 to repeat the verification process. If, on the other hand, the user does not want to retry verification, program control returns via the page connector 102 to FIGURE 4B at the page connector 88.

To download or upload a previously fingerprinted file, the steps shown in
15 FIGURE 4D are performed. To download a file from a peripheral computer to the central computer, the steps beginning at the page connector 120 are performed. First, the document file 22 selected by the user (at the block 180 in FIGURE 5 or at the block 180' in FIGURE 4B) is downloaded from the peripheral computer to the user's subscriber database 38 on the central computer, as indicated at the block 122. Next,
20 the downloaded document file 48 is checked at the blocks 124, 126 and 128 to determine whether the downloading was successful, i.e., error free. In particular, the file size and CRC of the downloaded document file 48 is calculated by the central computer at the block 124. The calculated data are then compared to the CRC and file size in the document activity log 28 on the peripheral computer, as indicated at the
25 block 126. At the decision diamond 128, a determination is made as to whether the data match. If the data do not match, the file downloading was unsuccessful. In this case, the downloaded document file 48 is deleted from the subscriber database 38 and an error message is sent at the block 132 to inform the user that the downloading was unsuccessful. The user is then given the opportunity to retry the downloading, as
30 indicated at the decision diamond 134. If the user decides not to retry downloading, program control is returned via the page connector 136 to FIGURE 4B at the page connector 90. On the other hand, if the user wants to retry downloading, program control loops back to the block 122 to repeat the downloading process.

If, at the decision diamond 128, a determination is made that the CRCs and
35 file sizes match, the file downloading was successful (i.e., error free). Then, at the blocks 127 and 129, the downloaded document file 48 is verified to ensure that the

-14-

downloaded document is identical to the document that was earlier fingerprinted (and date and time stamped). This ensures that only valid (i.e., verified) documents are downloaded and stored on the central computer. At the block 127, the CRC, file size, and date and time in the downloaded document file 48 are compared to the
5 corresponding data in the document record 46 generated when the file was fingerprinted. If the verification data do not match (determined at the decision diamond 129), the document file 48 is deleted from the subscriber database and an error message is sent, as indicated at the block 132. The user is then given a chance to retry downloading at the decision diamond 134, as previously described. If, on the
10 other hand, the verification data match, the downloaded file is valid and this result is recorded in the document activity log 28 on the peripheral computer and in the document record 46 in the subscriber database 38 on the central computer, as indicated at the block 130. Program control then returns via the page connector 136 to FIGURE 4B at the page connector 90.

15 To upload a file from the central computer to a peripheral computer, the steps beginning at the page connector 136 in FIGURE 4D are performed. First, the central computer searches the user's subscriber database 38 for the requested document (selected at the block 180 in FIGURE 5 or at the block 180' in FIGURE 4B), and uploads the document file 48 to the peripheral computer, as indicated at the
20 block 138. The uploaded document is then verified by comparing its CRC and size to that stored on the central computer. In particular, the file size and CRC of the uploaded document are calculated by the peripheral computer, as indicated at the block 140. The central computer then compares the file size and CRC calculated by the peripheral computer to the file size and CRC stored in the subscriber database 36
25 on the central computer, as indicated by the block 142. At the decision diamond 146, a determination is made as to whether the data match. If the data match, a record of the successful uploading is recorded in the document record 46 in the subscriber database 38 on the central computer and in the document activity log 24 on the peripheral computer, as indicated at the block 148. Program control then returns via
30 the page connector 136 to FIGURE 4B at the page connector 90.

If, on the other hand, at the decision diamond 146 a determination is made that the CRCs and file sizes do not match, an error message is sent to inform the user of this at the block 150 and the uploaded document is deleted from the peripheral computer. The user is then given the chance to retry uploading of the file, as
35 indicated by the decision diamond 152. If the user decides to retry uploading, program control loops back to the block 138 to restart uploading of the file. If, n

-15-

the other hand, the user decides not to reattempt uploading of the file, program control returns via the page connector 136 to FIGURE 4B at the page connector 90.

While the presently preferred embodiment of the invention has been illustrated and described, it will be appreciated that various changes can be made therein without departing from the spirit and scope of the invention. For example, while the fingerprint of a file was described as the CRC and size of the file, various other techniques could be used to uniquely identify the content of the file. Furthermore, while the fingerprint was said to be stored on both the peripheral and central computer, it may be more desirable not to store the fingerprint on the peripheral computer so that a user does not have access to this information. This would further reduce the risk of someone defeating the verification system. Furthermore, while the system has been entitled a digital verification system, it will be readily recognized by those skilled in the electronics art that the system could verify data stored in other forms, such as analog form. Thus, it will be understood that within the scope of the appended claims, various changes can be made in the specifically disclosed embodiments of the invention.

-16-

The embodiments of the invention in which an exclusive property or privilege is claimed are defined as follows:

1. A method of verifying computer files, including the steps of:
 - (a) generating a fingerprint of a computer file that is to be verified at a later time, said fingerprint being generated by a preselected technique such that said fingerprint is uniquely dictated by contents of said computer file;
 - (b) storing said fingerprint in a secured memory; and
 - (c) when verification of said computer file is desired:
 - (i) re-generating a fingerprint of said computer file using said preselected technique;
 - (ii) comparing said regenerated fingerprint to said stored fingerprint; and
 - (iii) if said regenerated fingerprint is the same as said stored fingerprint, then providing an indication that said computer file has not been altered or corrupted since generating said stored fingerprint, otherwise providing an indication that said computer file has been altered or corrupted since generating said stored fingerprint.
2. The method of claim 1, wherein said secured memory that stores said fingerprint is part of a central computer, and wherein said step of generating a fingerprint is performed by a peripheral computer interconnected to said central computer.
3. The method of claim 2, said method including verifying the date and time of creation of said computer file by performing steps including:
 - determining a date and time to assign to said computer file, said date and time indicative of when said computer file was created;
 - storing said date and time along with said stored fingerprint in said secured memory of said central computer; and
 - when verifying said computer file, reviewing said date and time stored in said secured memory.
4. The method of claim 3, wherein data is stored in said computer file in a digital format, further wherein said preselected technique of generating computer file fingerprints includes calculating the cyclic redundancy check value of a computer file,

-17-

so that said stored fingerprint and said regenerated fingerprint include cyclic redundancy check values.

5. The method of claim 4, wherein the user of said peripheral computer initiating said method must first identify himself, further wherein said fingerprint is stored in said secured memory in such a way that said user can be determined when said verification of said computer file is desired, so that the author of said computer file can be verified.

6. The method of claim 5, including the optional step of storing a copy of said computer file in said secured memory, so that if said computer file is deleted, altered or corrupted, said copy of said computer file can be retrieved from said secured memory.

7. The method of claim 3, wherein the user of said peripheral computer initiating said method must first identify himself, further wherein said fingerprint is stored in said secured memory in such a way that said user can be determined when said verification of said computer file is desired, so that the author of said computer file can be verified.

8. The method of claim 2, wherein data is stored in said computer file in a digital format, further wherein said preselected technique of generating computer file fingerprints includes calculating the cyclic redundancy check value of a computer file, so that said stored fingerprint and said regenerated fingerprint include cyclic redundancy check values.

9. The method of claim 2, wherein the user of said peripheral computer initiating said method must first identify himself, further wherein said fingerprint is stored in said secured memory in such a way that said user can be determined when said verification of said computer file is desired, so that the author of said computer file can be verified.

10. The method of claim 1, wherein data is stored in said computer file in a digital format, further wherein said preselected technique of generating computer file fingerprints includes calculating the cyclic redundancy check value of a computer file, so that said stored fingerprint and said regenerated fingerprint include cyclic redundancy check values.

-18-

11. The method of claim 10, wherein said preselected technique of generating computer file fingerprints further includes calculating the size of a computer file, so that said stored fingerprint and said regenerated fingerprint include file sizes.

12. The method of claim 1, said method including verifying the date and time of creation of said computer file by performing steps including:

determining a date and time to assign to said computer file, said date and time indicative of when said computer file was created;

storing said date and time along with said stored fingerprint in said secured memory of said central computer; and

when verifying said computer file, reviewing said date and time stored in said secured memory.

13. A method of verifying the date and time of creation of computer files, said method including the steps of:

(a) determining a date and time to assign to a computer file that is to be verified at a later time, said date and time indicative of when said computer file was created;

(b) storing said date and time in a secured memory; and

(c) when verification of the date and time of creation of said computer file is desired, reviewing said date and time stored in said secured memory.

14. The method of claim 13, wherein said date and time stored in said secured memory is also added to said computer file, and said reviewing of said date and time includes:

comparing said date and time stored in said secured memory and the date and time contained in said computer file; and

if said date and time stored in said secured memory and said date and time contained in said computer file are the same, then providing an indication that said date and time contained in said computer file is a valid indication of when said computer file was created, otherwise providing an indication that said date and time contained in said computer file is invalid.

15. The method of claim 14, wherein said secured memory is part of a central computer, and wherein said step of adding said date and time to said computer file is performed by a peripheral computer interconnected to said central computer.

16. The method of claim 15, wherein the user of said peripheral computer initiating said method must first identify himself, further wherein said date and time is stored in said secured memory in such a way that said user can be determined when said verification of the date and time of creation of said computer file is desired, so that the author of said computer file can be verified.

17. A computer file verifier for a multi-computer system including at least one peripheral computer, a central computer including secured memory, and an interface network interconnecting said at least one peripheral computer and said central computer, said computer file verifier comprising:

(a) a central computer program for execution on said central computer;

(b) a peripheral computer program for execution on said at least one peripheral computer, said central computer program and said peripheral computer program verifying computer files by performing the steps of:

(1) causing said peripheral computer to generate a fingerprint of a computer file that is to be verified at a later time, said fingerprint being generated by a preselected technique such that said fingerprint is uniquely dictated by contents of said computer file;

(2) causing said central computer to store said fingerprint in said secured memory of said central computer; and

(3) when verification of said computer file is desired:

(i) causing said peripheral computer to regenerate a fingerprint of said computer file using said preselected technique;

(ii) causing said central computer to compare said regenerated fingerprint to said stored fingerprint; and

(iii) if said regenerated fingerprint is the same as said stored fingerprint, causing said central computer to provide an indication that said computer file has not been altered or corrupted since generating said stored fingerprint, otherwise causing said central computer to provide an indication that said computer file has been altered or corrupted since generating said stored fingerprint.

18. The computer file verifier of claim 17, wherein said central computer program and said peripheral computer program also verify the date and time of creation of said computer file by performing the steps of:

-20-

causing said central computer to determine a date and time to assign to said computer file, said date and time indicative of when said computer file was created;

causing said central computer to store said date and time along with said stored fingerprint in said secured memory; and

when verifying said computer file, causing said central computer to review said date and time stored in said secured memory.

19. The computer file verifier of claim 18, wherein the user of said at least one peripheral computer initiating said peripheral computer program must first identify himself, further wherein said central computer program causes said central computer to store said fingerprint in said secured memory in such a way that said user can be determined when said verification of said computer file is desired, so that the author of said computer file can be verified.

20. The computer file verifier of claim 19, wherein said central computer optionally causes said central computer to store a copy of said computer file in said secured memory of said central computer, so that if said computer file is deleted, altered or corrupted, said copy of said computer file can be retrieved from said secured memory.

21. The method of claim 17, wherein data is stored in said computer file in a digital format, further wherein said preselected technique of generating computer file fingerprints includes calculating the cyclic redundancy check value of a computer file, so that said stored fingerprint and said regenerated fingerprint include cyclic redundancy check values.

22. The method of claim 21, wherein said preselected technique of generating computer file fingerprints further includes calculating the size of a computer file, so that said stored fingerprint and said regenerated fingerprint include file sizes.

23. The computer file verifier of claim 17, wherein the user of said at least one peripheral computer initiating said peripheral computer program must first identify himself, further wherein said central computer program causes said central computer to store said fingerprint in said secured memory in such a way that said user can be determined when said verification of said computer file is desired, so that the author of said computer file can be verified.

-21-

24. A computer file date and time verifier for a multi-computer system including at least one peripheral computer, a central computer including secured memory, and an interface network interconnecting said at least one peripheral computer and said central computer, said computer file verifier comprising:

(a) a central computer program for execution on said central computer; and

(b) a peripheral computer program for execution on said at least one peripheral computer, said central computer program and said peripheral computer program verifying the date and time of creation of computer files by performing the steps of:

(1) causing said peripheral computer to call said central computer to initiate date and time stamping of a computer file that is to be verified at a later time;

(2) causing said central computer to determine a date and time to assign to said computer file, said date and time indicative of when said computer file was created;

(3) causing said central computer to store said date and time in said secured memory; and

(4) when verification of the date and time of creation of said computer file is desired, causing said central computer to review said date and time stored in said secured memory.

25. The computer file date and time verifier of claim 24, wherein said peripheral computer program causes said peripheral computer to add said date and time stored in said secured memory to said computer file, and said step of causing said central computer to review said date and time in said secured memory comprises:

causing said central computer to compare said date and time stored in said secured memory and the date and time contained in said computer file; and

if said date and time stored in said secured memory and said date and time contained in said computer file are the same, then causing said central computer to provide an indication that said date and time contained in said computer file is a valid indication of when said computer file was created, otherwise causing said central computer to provide an indication that said date and time contained in said computer file is invalid.

-22-

26. The computer file date and time verifier of claim 25, wherein the user of said at least one peripheral computer initiating said peripheral computer program must first identify himself, further wherein said central computer program causes said central computer to store said date and time in said secured memory in such a way that said user can be determined when said verification of the date and time of creation of said computer file is desired, so that the author of said computer file can be verified.

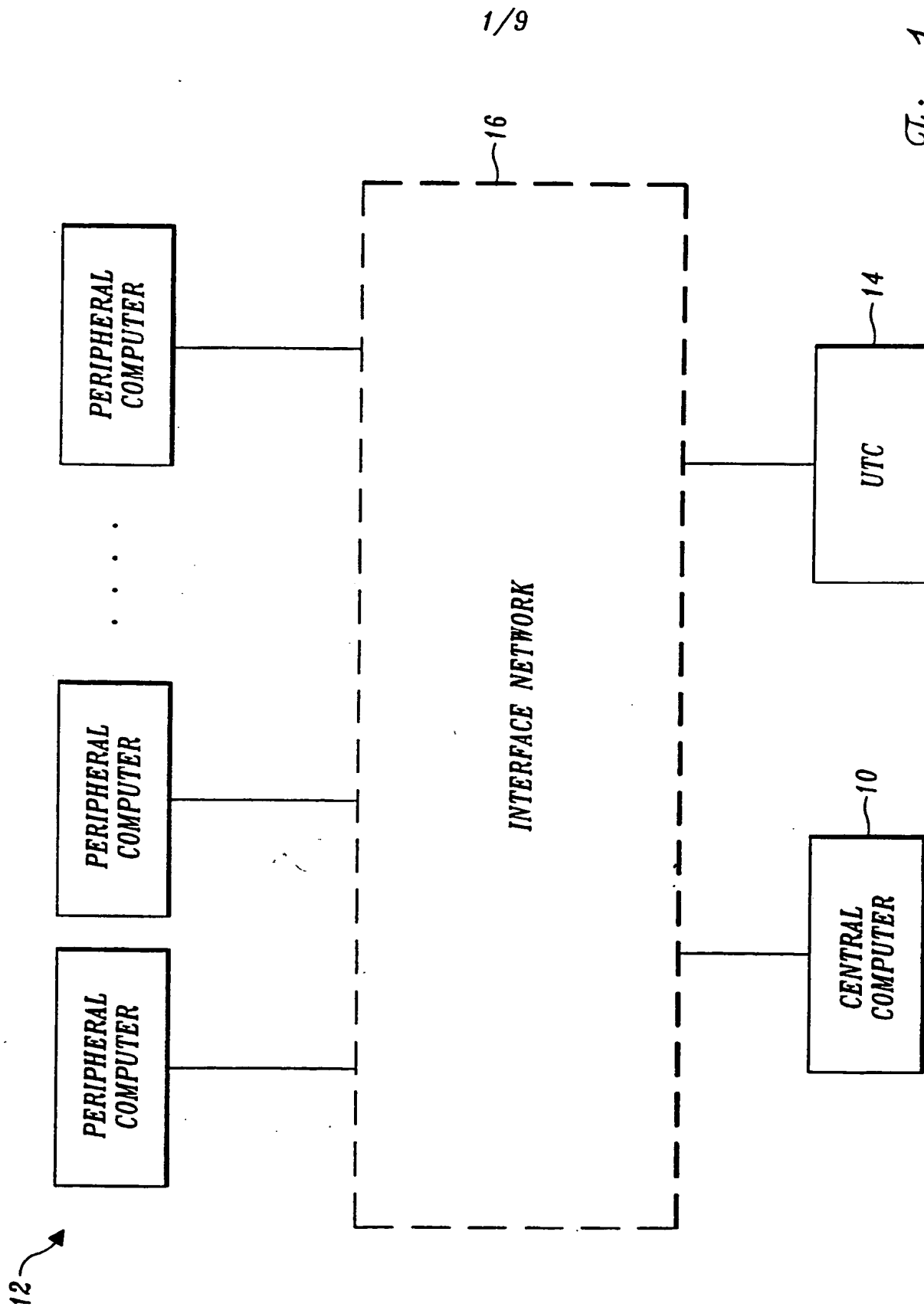


Fig. 1.

2/9

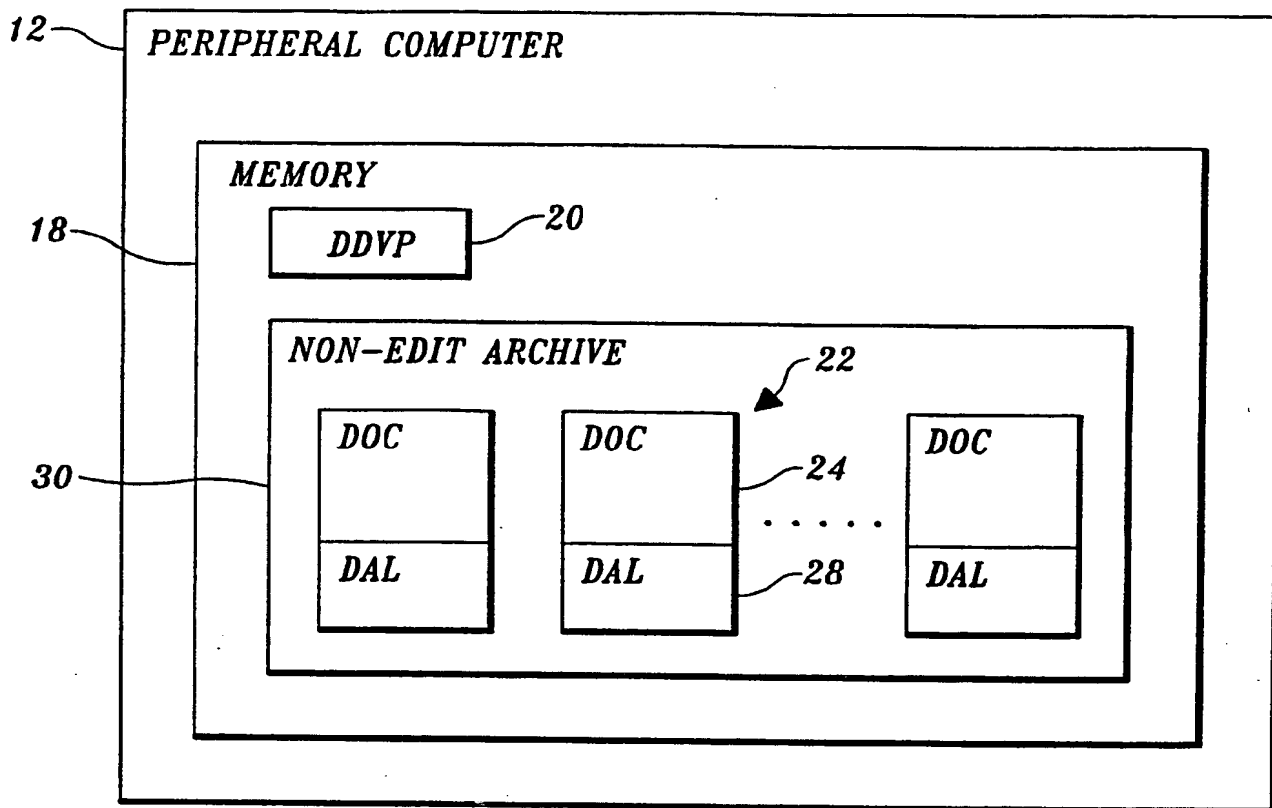


Fig. 2A.

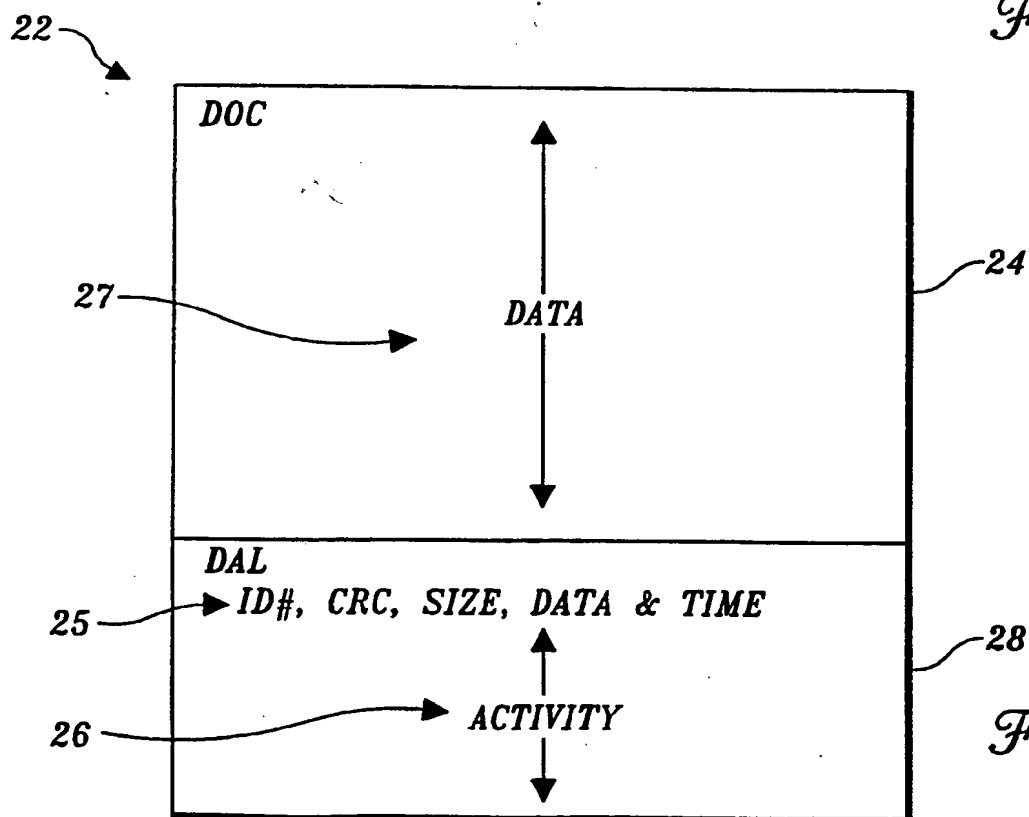


Fig. 2B.

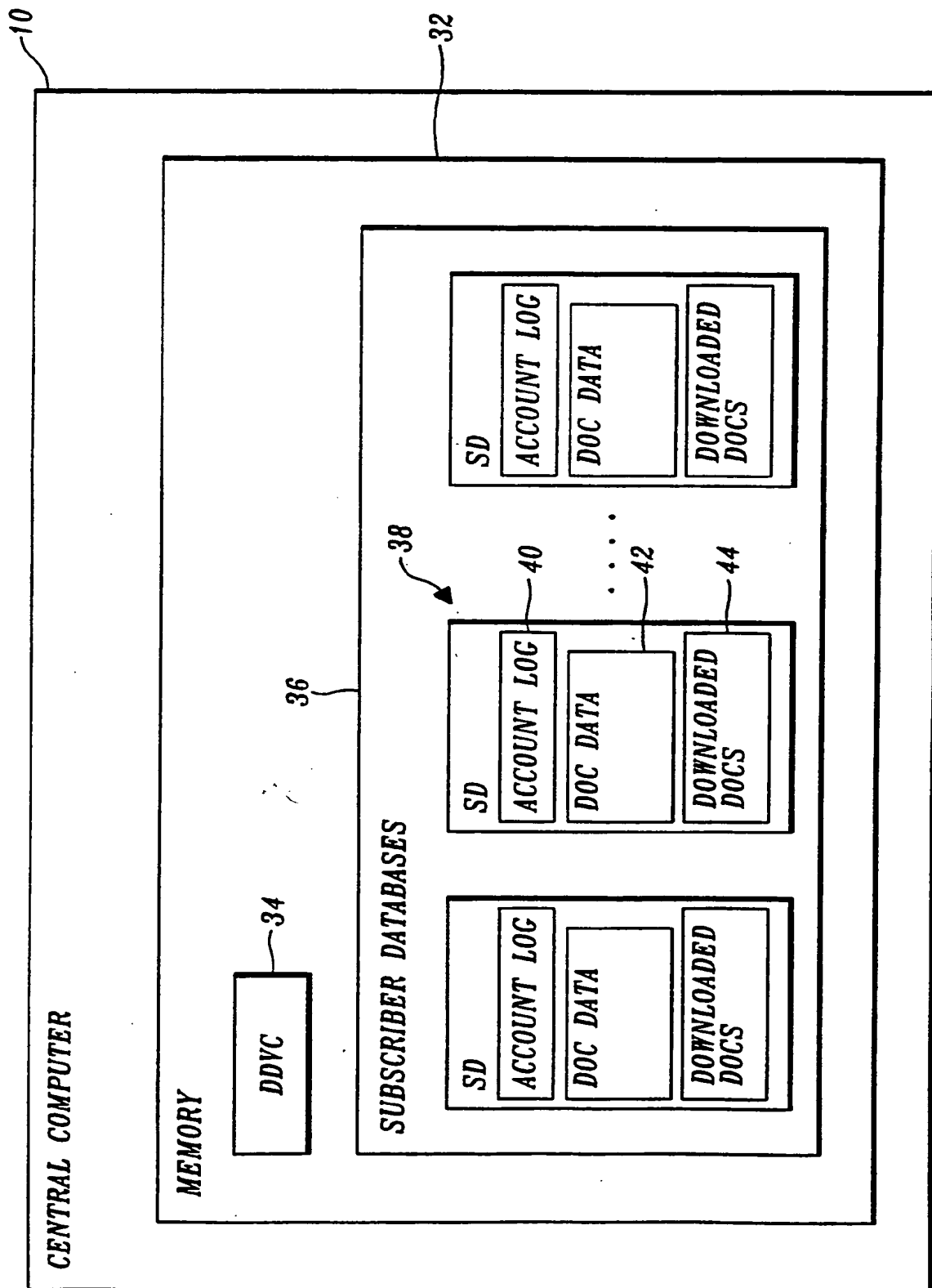


Fig. 3A.

4/9

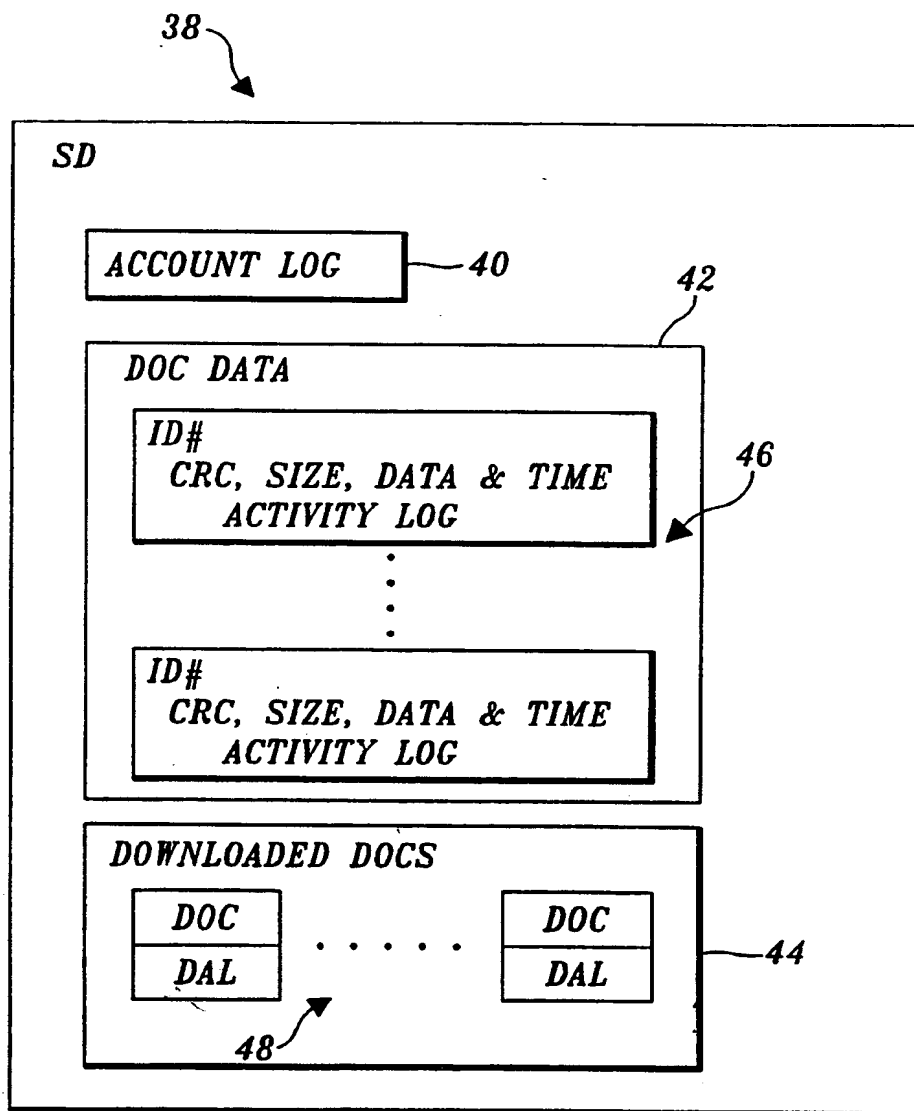
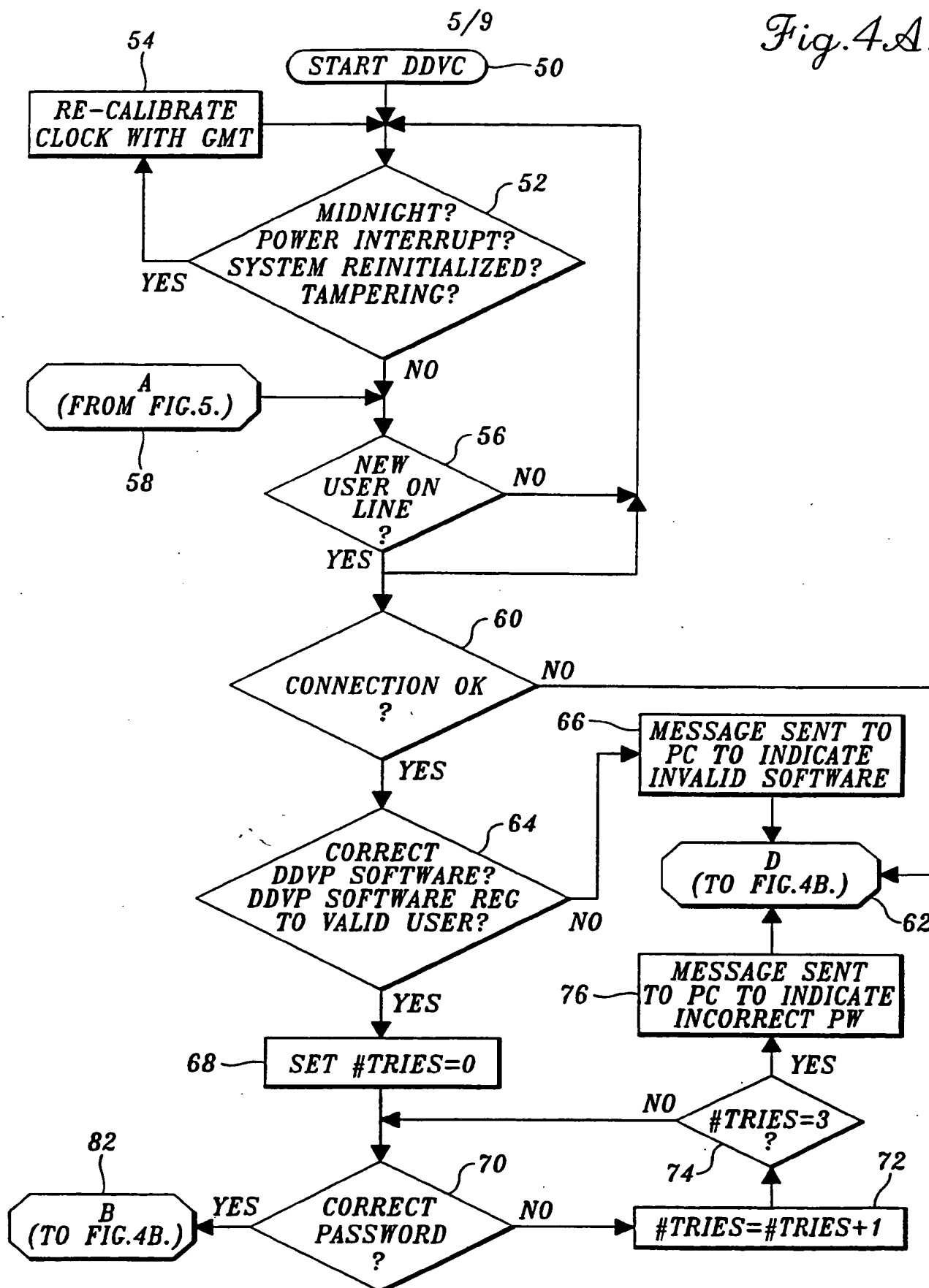
*Fig. 3B.*

Fig. 4A.



6/9

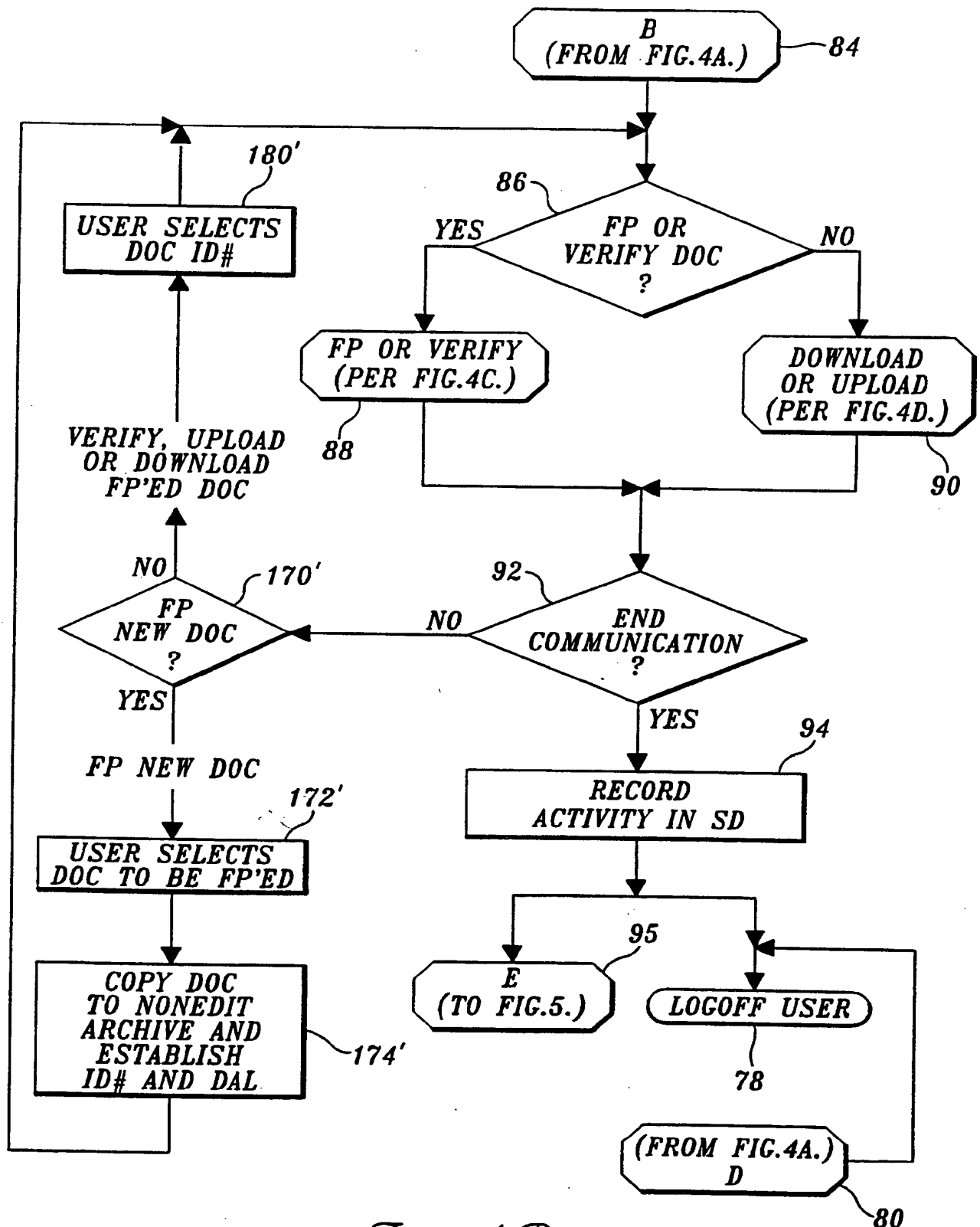


Fig. 4B.

7/9

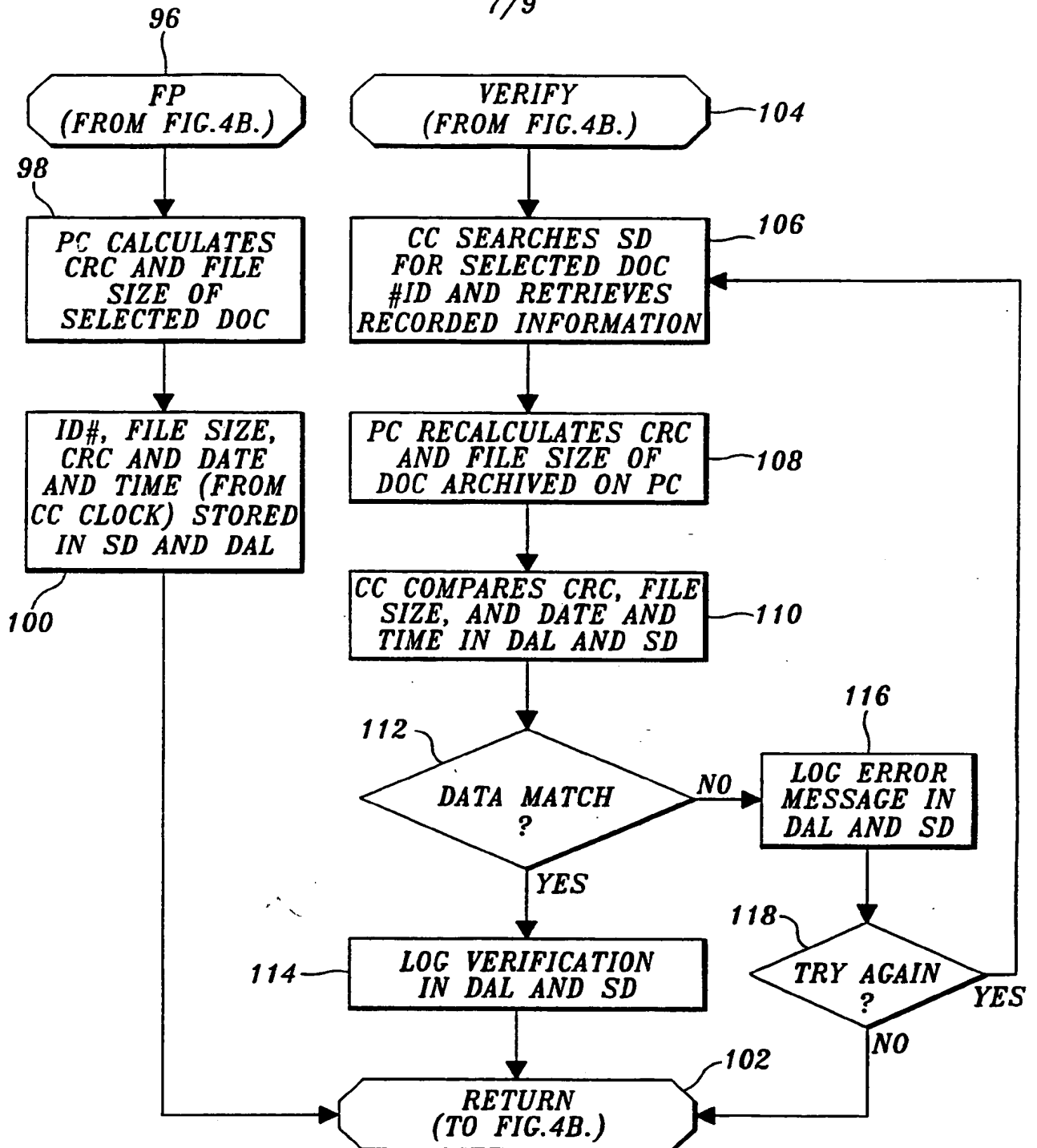


Fig. 4C.

8/9

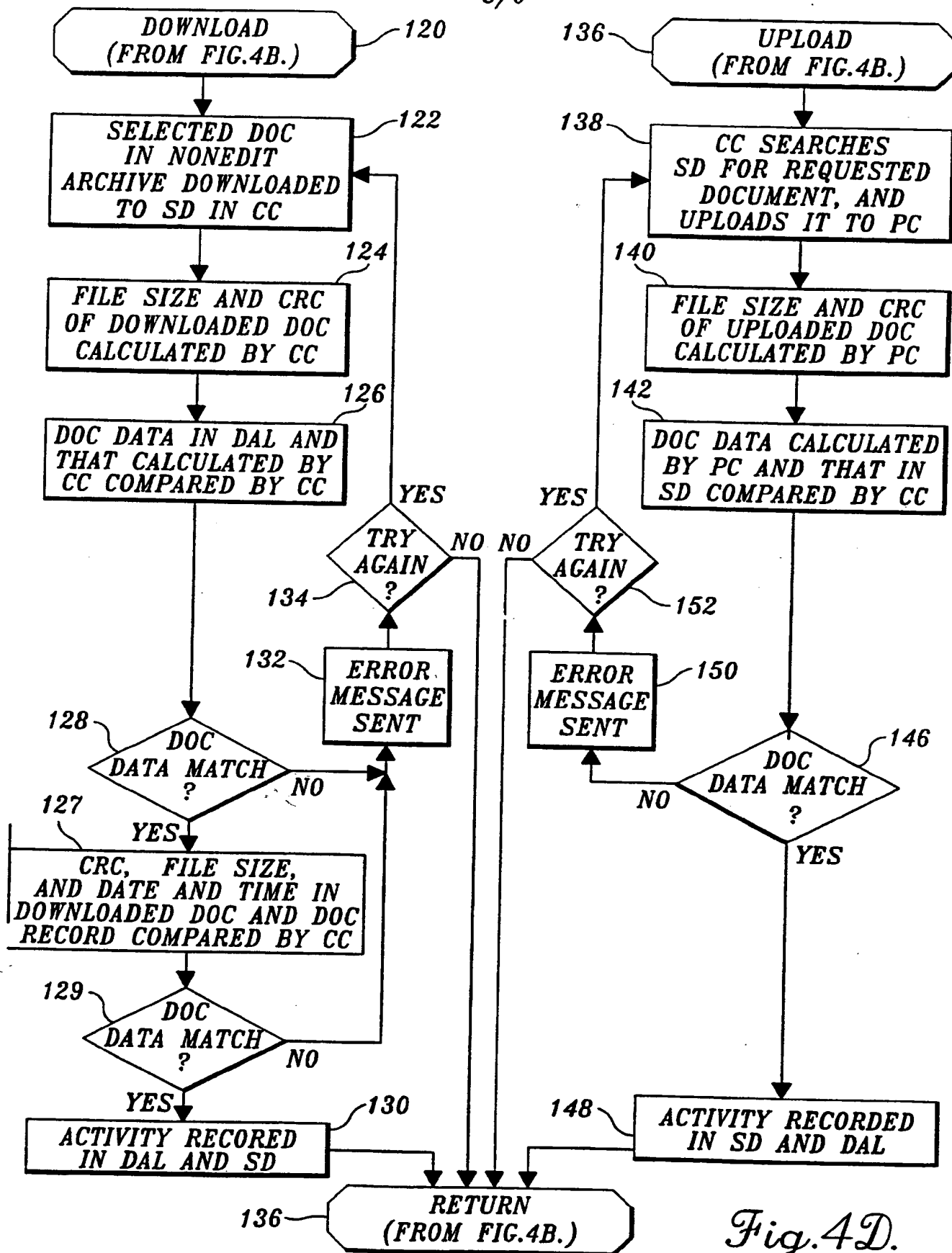


Fig.4D.

9/9

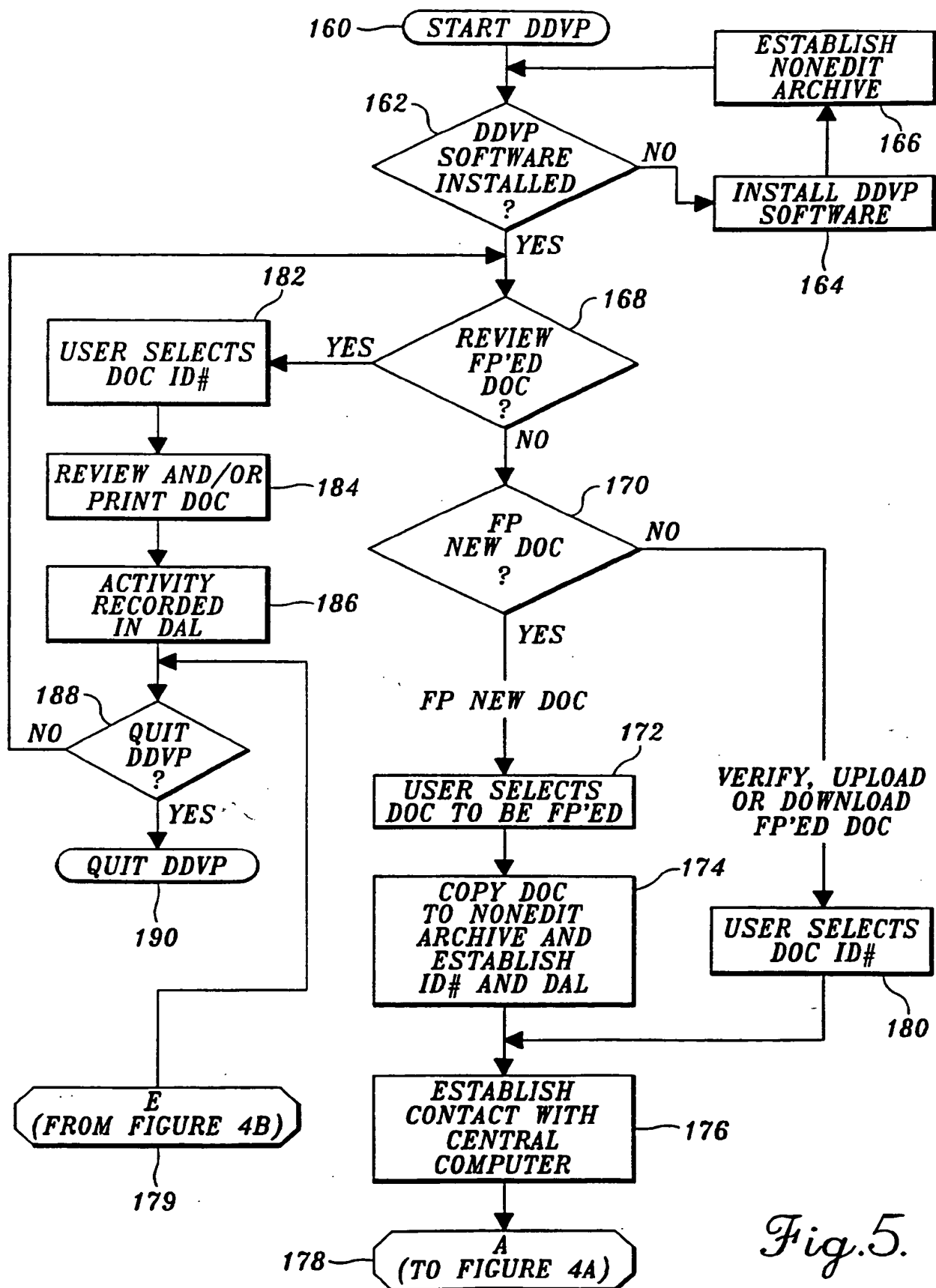


Fig. 5.

INTERNATIONAL SEARCH REPORT

International application No.:

PCT/US94/13360

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : G06F 7/02; H04L 9/32

US CL : 395/575

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/575; 364/408; 371/19; 380/4,23,25

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

Please See Extra Sheet.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ----- Y	US,A, 5,050,212 (DYSON) 17 September 1991; Abstract; col. 1, lines 47-67; and col. 5, line 37 to col. 6, line 66.	1 ----- 2-26
Y	US, A, 5,097,504 (CAMION ET AL) 17 March 1992, Abstract; Fig. 10; col. 10, line 28 to col. 13, line 22.	2-26
Y	Computers and Security, Volume 8, No. 7, issued November 1989, "How to Detect a Computer Virus in Your System", pages 557-561, especially page 558.	2-26
Y	Computers & Security, Volume 8, No. 6, issued October 1989, Dr. Harold Joseph Highland, "Random Bits & Bytes", pages 460-476, especially pages 469-471.	5, 7, 9, 16, 19, 23, 26

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents: "A" document defining the general state of the art which is not considered to be part of particular relevance "E" earlier document published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art "Z" document member of the same patent family	
--	--	--	--

Date of the actual completion of the international search

24 FEBRUARY 1995


Date of mailing of the international search report

04 MAY 1995

 Name and mailing address of the ISA/US
 Commissioner of Patents and Trademarks
 Box PCT
 Washington, D.C. 20231

Facsimile No. (703) 308-3230

Authorized officer


 V. Hua

Telephone No. (703) 305-9684

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US94/13360

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☒ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.
2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.
3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐
☐

- The additional search fees were accompanied by the applicant's protest.
No protest accompanied the payment of additional search fees.

B. FIELDS SEARCHED

Electronic data-bases consulted (Name of data base and where practicable terms used):

APS

search terms: verify? or valid? or authentic? or confirm?
 compare? or match?
 secure? or protect? or assure?
 file? or record? or data
 ?corrupt? or ?alter? or revise? or change? or modify? or vary or delete?
 fingerprint? or signature? or identification? or blueprint? or cyclic redundancy
 ?computer? or digital or ?process?

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING

This ISA found multiple inventions as follows:

This application contains the following inventions or groups of inventions which are not so linked as to form a single inventive concept under PCT Rule 13.1. In order for all inventions to be examined, the appropriate additional examination fees must be paid.

Group I, claim(s) 1-12 and 17-23, drawn to a method and an apparatus for verifying a computer file.

Group II, claim(s) 13-16 and 24-26, drawn to a method and an apparatus for verifying the date and the time indicating when a file was created.

The inventions listed as Groups I and II do not relate to a single inventive concept under PCT Rule 13.1 because, under PCT Rule 13.2, they lack the same or corresponding special technical features for the following reasons: The inventive concepts of Group I and Group II are only related as subcombinations which are disclosed as usable together in a single combination. The subcombinations, however, can be shown to be separately usable. In the instant case, the inventive concept of Group I has a separate utility such as for verifying a computer file without having to verify the date and the time indicating when the computer file was created.